INL/CON-07-13483
PREPRINT

Help for the Developers of Control System Cyber Security Standards

54th International Instrumentation Symposium

Robert P. Evans

May 2008

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Help for the Developers of Control System Cyber Security Standards

Robert P. Evans
Control System Security Program
Idaho National Laboratory

KEY WORDS:

Process Control System, Cyber Security, Standards

ABSTRACT

A *Catalog of Control Systems Security: Recommendations for Standards Developers* (Catalog), aimed at assisting organizations to facilitate the development and implementation of control system cyber security standards, has been developed. This catalog contains requirements that can help protect control systems from cyber attacks and can be applied to the Critical Infrastructures and Key Resources of the United States and other nations.

The requirements contained in the catalog are a compilation of practices or various industry bodies used to increase the security of control systems from both physical and cyber attacks. They should be viewed as a collection of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cyber security standards for control systems. The recommendations in the Catalog are intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cyber security standards specific to their individual security requirements.

INTRODUCTION

Protecting critical infrastructure is essential to the security, public health and safety, economic vitality, and way of life for a nation's citizens. Fundamental to the protection of critical infrastructure is ensuring the security of the systems that control this infrastructure. Developing and applying robust security standards enables control systems to be secured.

Development of security standards specific to critical infrastructure control systems is maturing, however, many standards lack the detailed guidance needed to ensure adequate protection from the emerging threats of cyber attacks on control systems. The *Catalog of Control Systems Security: Recommendations for Standards Developers* (Catalog) is specifically designed to provide various industry sectors the framework needed to develop sound security standards, guidelines, and best practices. These recommendations are not intended to replace the need for applying sound engineering judgment, best practices, and risk assessments. Decisions regarding when, where, and how these

Distributed with permission of author by ISA 2008
Presented at the 54th International Instrumentation Symposium

standards should be used are best decided by the specific industry sectors. The objective of the Catalog is to provide those decision makers with a common framework from which to draw requirements for securing control systems.

The term "control systems," as used throughout the Catalog, includes Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems, Distributed Control Systems (DCS), and other control systems specific to any of the critical infrastructure industry sectors. Although there are differences in these systems, their similarities enable a common framework for discussing and defining security requirements. As such, control system security standards are currently being developed by a variety of standards development groups to meet the needs of different industry sectors and regulatory environments. However, the requirements developed for a specific sector may not always be consistent or comparable with similar requirements developed in another sector. These developing standards often have differing emphases and levels of detail concerning specific security requirements.

The Catalog is intended to encompass these differences and provide a way to clarify security programs for control systems. Use of the Catalog is not limited to a specific industry sector. It should be viewed as a catalog of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cyber security standards for control systems.

Throughout the development of the Catalog, the following aspects of control systems were considered:

- **Proprietary Control System Technology** – A large percentage of control system hardware and software is proprietary. However, some vendors are moving toward marketing products that utilize non-proprietary, off-the-shelf technologies. Control system networks may also use proprietary or industry-specific protocols. The proprietary nature of control systems also requires professionals with system-specific knowledge to operate them.
- **Control System Equipment Life Cycle** – The life cycle for control system hardware is from 5 to 15 years (or more) as compared to the 2 to 3 year (or shorter) life cycle for information technology (IT) business systems. Building security into control system equipment has only started to appear. Legacy systems do not contain the standard security functionality as many IT systems such as encryption or logging.
- **Real Time Operation** – The systems that control critical infrastructure operations are designed and constructed to be in operation continuously. Any interruption in service may have catastrophic results to human life and property. This is another key difference between control systems and IT business systems and presents a unique challenge for securing these systems because security cannot compromise reliable operation.

The goal of a control system security program is to balance availability of the control system with security while operating within resource limits. When developing a security policy to address control systems, these characteristics must be considered. Security is not meant to impede operation and should be as transparent as possible. The most successful security program is one that integrates seamlessly and becomes a common aspect of daily operation. The intent of this document is to help facilitate such a program.

The Catalog was compiled by a team of cyber security professionals from several of the National Laboratories and the National Institute of Standards and Technology. The laboratories involved were

Argonne National Laboratory located in Argonne, Illinois, Idaho National Laboratory in Idaho Falls, Idaho, Oak Ridge National Laboratory in Oak Ridge Tennessee, Pacific Northwest National Laboratory located in Richland, Washington, and Sandia National Laboratories in Albuquerque, New Mexico. The National Institute of Standards and Technology is located in Gaithersburg, Maryland.

This was not only a multi-laboratory effort but a multi-disciplinary effort. The contributors brought experience from many different backgrounds which strengthened the product. This was a multi-year effort requiring cooperation between the contributing organizations and the Department of Homeland Security.

DOCUMENT OBJECTIVE

The Catalog is intended to assist organizations to ease the development and implementation of control system cyber security standards. It contains requirements that can help protect control systems from cyber attacks and is designed to be applicable to all types of organizations that use control systems to control processes.

The requirements contained in the Catalog should be viewed as a collection of recommendations to be considered and thoughtfully employed, as appropriate, when reviewing or developing cyber security standards for control systems. The recommendations are intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cyber security standards specific to their individual security requirements.

The Catalog is a grouping of requirements. Individually they are requirements that can be selected or not, modified or not, for use by an organization in developing a control system cyber security standard. Although it is recommended that all of the requirements be considered in developing a standard, their use is up to the body developing the standard.

INPUT DOCUMENT

The Catalog was developed using information obtained from eighteen documents, including standards, guidelines, reports, or recommended practices. Not all of these documents were used equally in the development of the Catalog, but all were considered. In many cases, these documents were still in draft condition. They represented various industry sectors including chemical, oil and natural gas, electrical, Federal, information technology, and cross-sector. The documents are listed below:

Chemical:

- Guidance for Addressing Cybersecurity in the Chemical Sector, Chemical Industry Data Exchange (CIDX)

Oil and Natural Gas

- Cryptographic Protection of SCADA Communications, AGA12-1 and 2, American Gas Association
- Pipeline SCADA Security, API 1164, American Petroleum Institute

- Security Guidelines for the Petroleum Industry, American Petroleum Institute Security

Electrical

- Guide for Electric Power Substation Physical and Electronic Security, IEEE 1402, Institute of Electrical and Electronics Engineers
- Critical Infrastructure Protection, NERC CIP-002-1 through CIP 009-1, North American Electric Reliability Council
- Security Guidelines for the Electricity Sector, North American Electric Reliability Council

Federal

- Security Requirements for Cryptographic Modules, FIPS 140-2, Federal Information Processing Standards Publication
- Recommended Security Controls for Federal Information Systems, NIST SP800-53, National Institute of Standards and Technology

Information Technology

- Code of Practice for Information Security Management, ISO/IEC 17799, International Organization for Standardization/ International Electrotechnical Commission
- Information Security Management Systems Requirements, ISO/IEC 27001, International Organization for Standardization/ International Electrotechnical Commission

Cross-Sector

- Data and Communication Security, IEC 62351, International Electrotechnical Commission
- Security for Industrial Automation and Control Systems, ANSI/ISA99.00.01 and .02, American National Standards Institute/ Instrumentation, Systems, and Automation Society
- Security Technologies for Manufacturing and Control Systems, ANSI/ISA-TR99.00.01-2004, American National Standards Institute/ Instrumentation, Systems, and Automation Society
- Integrating Electronic Security into the Manufacturing and Control Systems Environment, ANSI/ISA99.00.02-2004, American National Standards Institute/ Instrumentation, Systems, and Automation Society

The Catalog contains a cross-reference section which provides information on how the requirements in the Catalog relate to those in the other industry standards.

DOCUMENT SCOPE

The Catalog is intended to be a resource, not a standard. In many ways you could consider it a "wish book." At one time, when the *Sears Catalog* would come at Christmas, the children would look at all the toys and maybe wish for the train, a doll, or the cowboy set and then making out your letter to Santa. This is much the same concept. The idea is that the Catalog provides a single source from which a list of recommendations can selected for use in preparing requirements for a standard, therefore an organization only needs to consult a single source rather than sifting through the large collection of industry standards themselves.

The Catalog was designed to be applicable to all sectors. This is intended though to be control system specific. In order for the catalog to be useful to a wide variety of organizations, it of necessity must be very granular or general in nature. It is left to the organization to fill in specifics for their industry.

The Catalog is intended to be a living document that will be updated as information becomes available.

DOCUMENT STRUCTURE

The 219 requirements contained in the Catalog are divided into 18 groups or families based on the nature of the requirements. These families are:

Security Policy	Personnel Security	Organizational Security
Physical and Environmental Security	Systems and Services Acquisition	Configuration Management
Risk Management and Assessment	Planning	Systems and Communications Protection
Information and Document Management	Awareness and Training	Media Protection
Systems and Information Integrity	Access Control	Auditing and Accountability
Incident Response and Business Continuity	Monitoring and Reviewing Control System Monitoring Systems	Maintenance

Each family contains sufficient depth to be used in development of requirements. The families are not exclusive. There are requirements that could fall into several different families. In these cases the requirement, or a similar one, might appear in more than one family. The 219 requirements also contain a fair amount of depth, but because the Catalog is designed to address all sectors, they are not extremely specific. The intent of the Catalog to touch on a large number of topics, but only at a high level, therefore they will probably need to be modified for the specific industry. In most cases, the requirements should not be taken verbatim.

The requirements contained in the Catalog were derived by reviewing the requirements contained in various standards. Where several standards contained similar requirements, the team considered each and then came up with a requirement that might be a combination of all or might use the requirement that best fit the need. In some cases, new requirements were developed based on the experience of the team members.

Each requirement is divided into four parts: 1) the title of the requirement, 2) a statement of the requirement, normally a short description, 3) Supplemental Guidance which presents any additional information that might be helpful in understanding the intended scope of the requirement, and 4) Requirement Enhancement which is intended to give additional requirements should the system be considered critical. An example of one of the requirements is shown below:

Audit Reduction and Report Generation

Requirement. The control system provides an audit reduction and report generation capability.

Supplemental Guidance. Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records. Audit record processing must not degrade the operational performance of the control system. In general, audit record processing is not performed on the control system.

Requirement Enhancements. The control system provides the capability to automatically process audit records for events of interest based upon selectable event criteria.

GLOSSARY

Another important part of the Catalog is the Glossary. The Glossary identifies key terms used in cyber security and provides a listing of those terms with definitions. There are many other bodies, such as the Instrumentation, Systems and Automation Society, Institute of Electrical and Electronic Engineers, and Process Control Systems Forum, which also have lists of terms. No claim as to the strength of this glossary in comparison with the others. It does provide the terms in one location that can be easily used. Where these definitions were used from other sources, those sources are referenced.

CROSS REFERENCE

As indicated earlier in this paper, the Catalog also contains a cross-reference table showing how the requirements in the Catalog relate to requirements in other industry standard documents. Each of the requirements in the Catalog is listed and whether, in the viewpoint of the person providing information, other standards also address the requirement. Because of the way the analyses were performed, it is highly subjective in nature. These relationships have not been reviewed or approved by any of the standards bodies that created the standards. The cross reference still, however, gives an idea of the basic scope of the various standards that fed the Catalog and which requirements are of most concern to standards bodies.

The Cross Reference table, a sample of which is shown in Figure 1, consists of the Catalog requirements listed down one side of the table with the reference standards shown across the top. Where the reviewer believed that there was a correspondence, an “X” is placed in the table. This “X” then indicates that the referenced standard addresses, to some extent, the requirement in the Catalog.

Because of how quickly the reference standards evolve, this table will need to be maintained and updated. Even with its drawbacks, the cross reference can be very useful. For example, a manufacture trying to satisfy as many standards as possible can look at this table and determine which requirements are of most concern to the control system community. These requirements can then be addressed in the product.

		AGA12-1	AGA12-2	FIPS 140-2	API 1164/PI 1164	Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.1.1	**Error! Reference source not found.**	X	---	X	X	X	X	X	X	---	---	X	X	---	X	X
2.2.1	**Error! Reference source not found.**	---	---	---	X	---	X	X	X	---	---	X	X	---	X	---
2.2.2	**Error! Reference source not found.**	X	---	---	X	---	X	X	X	---	---	X	X	---	X	---
2.2.3	**Error! Reference source not found.**	---	---	---	X	---	X	X	X	---	---	X	X	---	---	---
2.2.4	**Error! Reference source not found.**	---	---	---	X	X	X	X	---	---	---	---	X	---	X	---
2.2.5	**Error! Reference source not found.**	---	---	---	X	X	X	X	---	---	---	---	X	---	X	---
2.2.6	**Error! Reference source not found.**	---	---	---	X	---	X	X	---	---	---	---	X	---	X	---
2.3.1	**Error! Reference source not found.**	---	---	---	X	X	X	X	X	---	---	---	X	X	X	X
2.3.2	Position Categorization	---	---	---	X	X	X	X	---	---	---	---	X	---	X	X
2.3.3	Personnel Screening	X	---	---	X	X	X	X	---	---	---	---	X	X	X	X
2.3.4	Personnel Termination	X	---	---	X	---	---	X	---	---	---	---	X	---	X	X

Figure 1. Sample of cross reference table.

CATALOG USAGE

The Catalog is not intended to be an exhaustive list of all requirements that could be associated with control system cyber security, but it can provide information to assist in developing a control system cyber security standard. The following are some ideas how the Catalog could be used to assist in standards development by providing:

- a checklist of items that should be considered in preparing a standard
- a single source for potential requirements
- a starting point for discussions on control system cyber security
- a glossary of terms that could be considered for inclusion in a standard.

The following paragraphs elaborate on each of the above items.

When preparing a standard, it is very easy to forget to include some topics that should be covered by the standard. The catalog, though not exhaustive in the requirements covered, does address the general topics that should be in a standard for control system cyber security. By going through each of the topics listed in the Catalog, the developer is forced to consider whether or not that topic is germane to the infrastructure for which the standard is being developed. If not, then it does not need to be included but the developer has to make a conscience decision as to the applicability of the topic. If it is a subject that needs to be covered, then there are recommendations for requirements that could be included. This method speeds up the development process by reducing the amount of background work that needs to be done by the developer. The developer still must be aware of what the infrastructure for which the standard is intended and be able to make informed decisions as to what types of requirements are necessary.

As discussed above, there are currently a great many documents in publication or in draft that present requirements aimed at protecting information technology or control systems from cyber intrusions. In order to determine what other organizations consider important in securing cyber systems, it would be necessary to go through each of these documents and look at each of the requirements or a person could use the Catalog which has essentially done the same thing. The Catalog contains a listing of requirements gleaned from the various documents and has combined those that are similar into a single requirement. In some cases, new requirements have been generated based on the authors' knowledge and experience. Each of these requirements can be used, if the standards developer chooses, in a new standard.

The standards development process begins with the key stakeholders in the organizations determining the scope of the standard. The families listed in the Catalog can provide a starting point for these discussions. By considering each of the families it can assist in helping determine which area the new standard should address.

The glossary can be used directly in a new standard, can be modified for the scope of the new standard, or can be used as a discussion enhancer to assist in the development process.

The above ideas are provided as a place to start and not an all-inclusive list of ways in which the Catalog can be used. As an organization considers the Catalog content, new methods of use will become clearer to the organization.

SUMMARY AND CONCLUSIONS

The catalog provides some basic ideas for an organization to consider in the development of cyber security standards for control systems. It is intended to be a resource for the development of standards and not a standard. It is envisioned that the Catalog can be used by both public and private sectors as a starting point to discuss and develop cyber security standards. It can be used to mitigate vulnerabilities that are identified by using the requirements. The catalog also covers organizational policies and procedures and can be used in setting up a control system management plan. It can also assist in training personnel.

It provides a shopping list of requirement for consideration in the development of a standard. Although not all of the requirements listed are applicable to all sectors, the Catalog still can provide a checklist of things to consider. By going through all of the requirements and asking "does this apply to what we are trying to do?" it will make for a more complete standard.

The Catalog identifies and consolidates recommended practices from multiple cyber security standards into a set of uniform recommendations. It is intended to be a living document requiring regular updates.

This work was funded by the United States Department of Homeland Security, through the Control System Security Program of the National Cyber Security Division.

REFERENCES

The following documents were used in the preparation of the Catalog. They are listed in alphabetical order.

American Gas Association, Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan (AGA 12, Part 1), March 14, 2006.

American Gas Association, Cryptographic Protection of SCADA Communications Part 2: Retrofit link encryption for asynchronous serial communications (AGA 12, Part 2), March 31, 2006.

American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.01-2004), Security Technologies for Manufacturing and Control Systems, 11 March 2004

American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.02-2004), Integrating Electronic Security into the Manufacturing and Control Systems Environment, 12 April 2004

American Petroleum Institute, API 1164: Pipeline SCADA Security, First Edition, September, 2004.

American Petroleum Institute, Security Guidelines for the Petroleum Industry, April 2005

Chemical Industry Data Exchange, Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1, May 2005 (Note: This document has been superseded by Guidance for Addressing Cybersecurity in the Chemical Sector, Version 3.0, Chemical Sector Cyber Security Program, May 2006).

Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, Issued May 25, 2001, Updated December 03, 2002.

International Electrotechnical Commission 62351, Data and Communication Security, Draft.

Institute of Electrical and Electronics Engineers 1402, Guide for Electric Power Substation Physical and Electronic Security, January 30, 2000.

Instrumentation, Systems, and Automation Society Standards Committee, DRAFT dISA-99.00.01 Manufacturing and Control Systems Security Part: Concepts, Models and Terminology Draft 2, Edit 3 October 2005

Instrumentation, Systems, and Automation Society Standards Committee, DRAFT dISA-99.00.02 Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program, Draft 1, Edit 5 September 20, 2005

National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Revision 1 Final Public Draft, October, 2006.

North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-1 through CIP 009-1), May 2006.

North American Electric Reliability Council, Security Guidelines for the Electricity Sector, Version 1.0, June 14, 2002.